Configuring SGM Security

This chapter provides the following information about configuring SGM security and limiting access to SGM:

- Configuring SGM User-Based Access, page 18-1
- Implementing SSL Support in SGM, page 18-26
- Limiting SGM Client Access to the SGM Server (Solaris Only), page 18-40

Configuring SGM User-Based Access

SGM enables you to control who is allowed to do what in SGM, beyond simply specifying root and non-root users. SGM calls this ability User-Based Access.

User-Based Access provides multi-level password-protected access to SGM features. Each user can have a unique user name and password. Each user can also be assigned to one of five levels of access, which control the list of SGM features accessible by that user.

To configure SGM User-Based Access, perform the tasks in the following sections. Required and optional tasks are indicated.

- Implementing SGM User-Based Access (Solaris Only), page 18-2 (Required)
- Creating Secure Passwords, page 18-5 (Required)
- Configuring SGM User Authentication Levels (Solaris Only), page 18-6 (Required)
- Automatically Disabling Users and Passwords (Solaris Only), page 18-10 (Optional)

Implementing SGM User-Based Access (Solaris Only)

Before you can access SGM's full suite of security commands, you must enable SGM User-Based Access, configure the type of security authentication you want to use, and begin adding users to your authentication lists.

To implement SGM User-Based Access, use the following procedure:

Step 1   Log in as the root user, as described in the "Becoming the Root User (Solaris Only)" section on page 2-3, or as a super user, as described in the "Specifying a Super User (Solaris Only)" section on page 18-24.

Step 2   Enter the following commands:

 # cd /opt/CSCOsgm/bin

 # ./sgm useraccess enable

SGM User-Based Access is enabled the next time you restart the SGM server.

Step 3 If you have already configured the type of SGM security authentication you want to use, skip to Step 4.

Otherwise, configure the type of SGM security authentication you want to use:

- *Local authentication* allows you to create user accounts and passwords local to the SGM system. When using this method, you can use SGM User-Based Access commands manage user names, passwords, and access levels.

  To enable local authentication, enter the following command:

  # ./sgm authtype local

- *Solaris authentication* uses standard Solaris-based user accounts and passwords, as specified in the */etc/nsswitch.conf* file. Authentication can be provided by the local */etc/passwd* file or from a distributed Network Information Services (NIS) system. You can use all SGM User-Based Access commands except the following commands:

  - **sgm disablepass**

  - **sgm passwordage**

  - **sgm userpass**

  You must use Solaris commands, such as **passwd**, to manage passwords.

  Users also cannot change their passwords using the SGM client. Instead, they must manage their passwords on the external authentication servers, using Solaris commands, such as **passwd**.

  All new passwords take effect the next time SGM automatically synchronizes local SGM passwords with Solaris, or you can manually synchronize passwords at any time using the **sgm syncusers** command.

  In addition, if you have enabled Solaris authentication, you must be logged in as the root user, not a super user, to use the following SGM commands:

  - **sgm adduser**

  - **sgm disableuser**

  - **sgm enableuser**

  - **sgm updateuser**

To enable Solaris authentication, enter the following command:

 # ./sgm authtype solaris

See the "SGM Command Reference" section on page C-1 for more information on the use of each of the above SGM commands.

Step 4 To add a user to your SGM User-Based Access authentication list, use the following command:

 # ./sgm sgm adduser *username*

where *username* is the name of the user.

✎

Note If **sgm authtype** is set to **solaris**, you must be logged in as the root user, not as a super user, to enter this command.

SGM also prompts you for the authentication level for the user. Valid levels are:

- **1**—Basic User
- **2**—Power User
- **3**—Network Operator
- **4**—Network Administrator
- **5**—System Administrator

For more information about authentication levels, see the "Configuring SGM User Authentication Levels (Solaris Only)" section on page 18-6.

If **sgm authtype** is set to **local**, SGM also issues the following prompts:

- SGM prompts you for the user's password. When setting the password, follow the rules and considerations in the "Creating Secure Passwords" section on page 18-5.

- SGM asks whether you want to force the user to change the password at the next login. The default is not to force the user to change the password.

(Whenever a user needs to change a password, SGM issues an appropriate message and prompts for the user name and new password.)

> ✎
>
> **Note**   If **sgm authtype** is set to **solaris**, users cannot change their passwords
> using the SGM client. Instead, they must manage their passwords on the
> external authentication servers, using Solaris commands, such as **passwd**.
> All new passwords take effect the next time SGM automatically
> synchronizes local SGM passwords with Solaris, or you can manually
> synchronize passwords at any time using the **sgm syncusers** command.
> See the "sgm syncusers" section on page C-118 for more information.

At this point, you have implemented your basic SGM User-Based Access. Users
must now log in before using the SGM client, the GTT client, and SGM
Web-based functions. Use the remaining procedures in this section to customize
your SGM security system.

> ✎
>
> **Note**   After you implement SGM User-Based Access, if a user logs in on one SGM or
> GTT client, then logs in on a second SGM or GTT client, SGM closes the first
> client and records the event in the system security log.

Creating Secure Passwords

When setting passwords in SGM, keep in mind the following rules and
considerations:

- The password must be at least 6 characters, up to an unlimited number of
  characters. However, passwords longer than 15 characters are not
  recommended.

- The password cannot be identical to the user name.

- The new password cannot be the same as the old password.

- SGM does not allow users to switch back-and-forth between two passwords.

- The password cannot be a common word. SGM uses the dictionary located at */usr/lib/share/dict/words* to determine whether a word is common. To override the SGM dictionary, change the DICT_FILE entry in the *System.properties* file:

  – To disable the SGM dictionary and allow common words, change the DICT_FILE entry to:

     DICT_FILE=/dev/null

  – To use a custom dictionary, change the DICT_FILE entry to:

     DICT_FILE=/*new-dictionary*

  where *new-dictionary* is the path and filename of the custom dictionary file, such as **/users/rolive/words**. Each line in the custom dictionary must contain a single word, with no leading or trailing spaces.

Configuring SGM User Authentication Levels (Solaris Only)

This section describes the user authentication levels in SGM, and the SGM functions and Web displays available at each level:

- Basic User (Level 1) Access, page 18-7
- Power User (Level 2) Access, page 18-8
- Network Operator (Level 3) Access, page 18-8
- Network Administrator (Level 4) Access, page 18-9
- System Administrator (Level 5) Access, page 18-9

The authentication level that includes a function is the *lowest* level with access to that function. The function is also available to all higher authentication levels. For example, a System Administrator also has access to all Network Administrator functions.

Authentication levels are based on the function to be performed, not on the target object. Therefore, if a user can perform a function on one SGM object (such as deleting a node), the user can perform the same function on all similar SGM objects (such as deleting a signaling point or linkset).

> **Note**   Access to SGM information and downloads on Cisco.com is already protected by Cisco.com, and is not protected by SGM.

To configure the authentication level for a user, use the **sgm adduser** command, as described in the "Implementing SGM User-Based Access (Solaris Only)" section on page 18-2, or the **sgm updateuser** or **sgm newlevel** command, as described in the "Enabling and Changing Users and Passwords (Solaris Only)" section on page 18-16.

Basic User (Level 1) Access

Basic Users can view SGM data, load SGM files, and use SGM drill-down menus.

Basic Users have access to the following SGM functions:

- Connecting to a new server
- Applying changes to views
- Loading the DEFAULT view and existing views, but not saving them
- Editing, loading, and applying preferences files, but not saving them
- Viewing and manipulating the topology map, and saving it as a JPEG, but not saving icon locations
- Viewing network objects, events, details, and notes
- Viewing the ITP home page
- Loading existing event filters, but not saving them
- Printing SGM windows
- Launching CiscoWorks2000

Basic Users have access to the following SGM Web displays:

- Server Home Page
- System README
- Network Status

- System Data Files
  - Notes
  - Views
  - Preferences
- Viewing SGM documentation
- Downloading client software

Power User (Level 2) Access

Power Users have access to all Basic User functions.

Power Users can change some aspects of the way SGM works.

Power Users have access to the following SGM functions:

- Editing network objects, events, and views
- Unignoring network objects and views
- Saving preferences files, event filters, and views
- Acknowledging events
- Viewing ITP real-time data and charts
- Viewing the event configuration, but not editing it

Power Users have access to the following SGM Web displays:

- System Status, excluding User Accounts and System Troubleshooting
- Accounting Statistics Reports
- Network Statistics Reports

Network Operator (Level 3) Access

Network Operators have access to all Basic User and Power User functions.

Network Operators can make changes to SGM network files.

Network Operators have access to the following SGM functions:

- Ignoring network objects and views
- Polling nodes

- Telnetting to the ITP
- Viewing route table files and GTT files, but not editing them

Network Operators have access to the following SGM Web displays:

- Point Code Inventories
- System Data Files
    - Route table files
    - Global Title Translation (GTT) table files
    - System ITP IOS README

Network Administrator (Level 4) Access

Network Administrators have access to all Basic User, Power User, and Network Operator functions.

Network Administrators have access to all SGM client functions.

Network Administrators have access to the following SGM functions:

- SNMP configuration
- Network Discovery
- Deleting network objects
- Managing and unmanaging nodes
- Editing and saving route table files and GTT files
- Using the Deployment Wizard

Network Administrators have access to the following SGM Web displays:

- System Data Files: Discovery Seeds

System Administrator (Level 5) Access

System Administrators have access to all Basic User, Power User, Network Operator, and Network Administrator functions.

System Administrators have access to all functions in SGM.

System Administrators have access to the following SGM Web displays:

- System Messages and Logs
- System Status, including User Accounts and System Troubleshooting
- Trap Host Configuration, including SNMP configuration information
- System Information
  - System Command Log
  - System Console Log
  - System Event Automation Log
  - System Install Log
  - System Process Services
  - System Properties
  - System Report Parameters and Timers Page
  - System Reports Log
  - System Root Variables
  - System Security Log
  - System Web Access Log
  - System Web Error Log

Automatically Disabling Users and Passwords (Solaris Only)

After you have implemented the basic SGM User-Based Access security system, you can customize the system to automatically disable users and passwords when certain conditions are met.

To automatically disable users and passwords, use the following procedures:

Step 1   Log in as the root user, as described in the "Becoming the Root User (Solaris Only)" section on page 2-3, or as a super user, as described in the "Specifying a Super User (Solaris Only)" section on page 18-24.

Step 2   Enter the following command:

 # cd /opt/CSCOsgm/bin

Step 3   (Optional) You can configure SGM to generate an alarm after a specified number of unsuccessful login attempts by a user. To do so, enter the following command:

 # ./sgm badloginalarm *number-of-attempts*

where *number-of-attempts* is the number of unsuccessful login attempts allowed before SGM generates an alarm.

The valid range is 1 unsuccessful attempt to an unlimited number of unsuccessful attempts. The default value is 5 unsuccessful attempts.

To disable this function (that is, to prevent SGM from automatically generating an alarm after unsuccessful login attempts), enter the following command:

 # ./sgm badloginalarm clear

Step 4   (Optional) You can configure SGM to disable a user's security authentication automatically after a specified number of unsuccessful login attempts. To do so, enter the following command:

 # ./sgm badlogindisable *number-of-attempts*

where *number-of-attempts* is the number of unsuccessful login attempts allowed before SGM disables the user's authentication. SGM does not delete the user from the authentication list, SGM only disables the user's authentication.

The valid range is 1 unsuccessful attempt to an unlimited number of unsuccessful attempts. The default value is 10 unsuccessful attempts.

To re-enable the user's authentication, use the **sgm enableuser** command.

To disable this function (that is, to prevent SGM from automatically disabling a user's authentication after unsuccessful login attempts), enter the following command:

 # ./sgm badlogindisable clear

Step 5   (Optional) SGM keeps track of the date and time each user last logged in. You can configure SGM to disable a user's security authentication automatically after a specified number of days of inactivity. To do so, enter the following command:

> **# ./sgm inactiveuserdays** *number-of-days*

where *number-of-days* is the number of days a user can be inactive before SGM disables the user's authentication. SGM does not delete the user from the authentication list, SGM only disables the user's authentication.

The valid range is 1 day to an unlimited number of days. There is no default setting.

To re-enable the user's authentication, use the **sgm enableuser** command.

This function is disabled by default. If you do not specify the **sgm inactiveuserdays** command, user accounts are never disabled as a result of inactivity.

If you have enabled this function and you want to disable it (that is, to prevent SGM from automatically disabling user accounts as a result of inactivity), enter the following command:

> **# ./sgm inactiveuserdays clear**

Step 6   (Optional) If **sgm authtype** is set to **local**, you can configure SGM to force users to change their passwords after a specified number of days.

To configure SGM to force users to change their passwords after a specified number of days, enter the following command:

> **# ./sgm passwordage** *number-of-days*

where *number-of-days* is the number of days allowed before users must change their passwords.

The valid range is 1 day to an unlimited number of days. There is no default setting.

This function is disabled by default. If you do not specify the **sgm passwordage** command, users never need to change their passwords.

If you have enabled this function and you want to disable it (that is, prevent SGM from forcing users to change passwords), enter the following command:

> **# ./sgm passwordage clear**

> ✎
>
> **Note**   If **sgm authtype** is set to **solaris**, you cannot use the **sgm passwordage** command. Instead, you must manage passwords on the external authentication servers.

Step 7   (Optional) You can configure SGM to disconnect an SGM or GTT client automatically after a specified number of minutes of inactivity. To do so, enter the following command:

> **# ./sgm clitimeout** *number-of-minutes*

where *number-of-minutes* is the number of minutes an SGM or GTT client can be inactive before SGM disconnects the client.

The valid range is 1 minute to an unlimited number of minutes. There is no default value.

This function is disabled by default. If you do not specify the **sgm clitimeout** command, clients are never disconnected as a result of inactivity.

If you have enabled this function and you want to disable it (that is, never disconnect a client as a result of inactivity), enter the following command:

> **# ./sgm clitimeout clear**

Manually Disabling Users and Passwords (Solaris Only)

As described in the "Automatically Disabling Users and Passwords (Solaris Only)" section on page 18-10, you can customize SGM to automatically disable users and passwords when certain conditions are met. However, you can also manually disable SGM User-Based Access users and passwords when the need arises. To do so, use the following procedures:

Step 1   Log in as the root user, as described in the "Becoming the Root User (Solaris Only)" section on page 2-3, or as a super user, as described in the "Specifying a Super User (Solaris Only)" section on page 18-24.

Step 2   Enter the following command:

> **# cd /opt/CSCOsgm/bin**

Step 3   (Optional) To delete a user entirely from the SGM User-Based Access authentication list, enter the following command:

> **# ./sgm deluser** *username*

where *username* is the name of the user.

If you later decide to add the user back to the authentication list, you must use the **sgm adduser** command.

Step 4   (Optional) If **sgm authtype** is set to **local**, you can disable a user's password. To do so, enter the following command:

> **# ./sgm disablepass** *username*

where *username* is the name of the user. SGM does not delete the user from the authentication list, SGM only disables the user's password.

> ✎
>
> **Note**   If **sgm authtype** is set to **solaris**, you cannot use the **sgm disablepass** command. Instead, you must manage passwords on the external authentication servers.

The user must change his password the next time he logs in.

You can also re-enable the user's authentication with the same password, or with a new password:

- To re-enable the user's authentication with the same password as before, use the **sgm enableuser** command.

- To re-enable the user's authentication with a new password, use the **sgm userpass** command.

Step 5   (Optional) To disable a user's authentication, but not the user's password, use the following command:

> **# ./sgm disableuser** *username*

where *username* is the name of the user.

✎

Note   If **sgm authtype** is set to **solaris**, you must be logged in as the root user, not as a super user, to enter this command.

SGM does not delete the user from the authentication list, SGM only disables the user's authentication. The user cannot log in until you re-enable the user's authentication:

- To re-enable the user's authentication with the same password as before, use the **sgm enableuser** command.

- To re-enable the user's authentication with a new password, use the **sgm userpass** command.

Enabling and Changing Users and Passwords (Solaris Only)

Of course, SGM also enables you to re-enable users and passwords, and change user accounts. To enable and change users and passwords, use the following procedures:

Step 1   Log in as the root user, as described in the "Becoming the Root User (Solaris Only)" section on page 2-3, or as a super user, as described in the "Specifying a Super User (Solaris Only)" section on page 18-24.

Step 2   Enter the following command:

 # cd /opt/CSCOsgm/bin

Step 3   (Optional) To re-enable a user's authentication, which had been disabled either automatically by SGM or by a super user, enter the following command:

 # ./sgm enableuser *username*

where *username* is the name of the user. SGM re-enables the user's authentication with the same password as before.

> **Note**   If **sgm authtype** is set to **solaris**, you must be logged in as the root user, not as a super user, to enter this command.

Step 4   (Optional) If **sgm authtype** is set to **local**, you can change a user's password, or re-enable the user's authentication with a new password, if the user's authentication had been disabled either automatically by SGM or by a super user. To change a password or to re-enable a user's authentication with a new password, enter the following command:

 # ./sgm userpass *username*

where *username* is the name of the user.

SGM prompts you for the new password. When setting the password, follow the rules and considerations in the "Creating Secure Passwords" section on page 18-5.

If the user's authentication has also been disabled, SGM re-enables the user's authentication with the new password.

> ✎
>
> **Note**   If **sgm authtype** is set to **solaris**, you cannot use the **sgm userpass**
>   command. Instead, you must manage passwords on the external
>   authentication servers.

Step 5   (Optional) To change a user's authentication level and password, enter the
             following command:

> **# ./sgm updateuser** *username*

where *username* is the name of the user.

> ✎
>
> **Note**   If **sgm authtype** is set to **solaris**, you must be logged in as the root user,
>   not as a super user, to enter this command.

SGM prompts you for the new authentication level. Valid levels are:

- **1**—Basic User
- **2**—Power User
- **3**—Network Operator
- **4**—Network Administrator
- **5**—System Administrator

For more information about authentication levels, see the "Configuring SGM User
Authentication Levels (Solaris Only)" section on page 18-6.

If **sgm authtype** is set to **local**, SGM also prompts you for the user's new
password. When setting the password, follow the rules and considerations in the
"Creating Secure Passwords" section on page 18-5.

Step 6   (Optional) To change a user's authentication level, but not the user's password, enter the following command:

> **# ./sgm newlevel** *username*

where *username* is the name of the user.

SGM prompts you for the new authentication level. Valid levels are:

- **1**—Basic User

- **2**—Power User

- **3**—Network Operator

- **4**—Network Administrator

- **5**—System Administrator

For more information about authentication levels, see the "Configuring SGM User Authentication Levels (Solaris Only)" section on page 18-6.

Displaying a Message of the Day

SGM enables you to display a user-specified SGM system notice called the message of the day (Figure 18-1). You can use the message of the day to inform users of important changes or events in the SGM system. The message of the day also gives users an opportunity to exit the SGM or GTT client before launching.

If the message of the day is enabled, it is displayed whenever a user attempts to launch an SGM or GTT client:

- If the user accepts the message, the client launches.

- If the user declines the message, the client does not launch.

To display the Message of the Day dialog, use one of the following procedures:

- Launch the SGM or GTT client. If there is a message of the day, the Message of the Day dialog is displayed.

- Select **View > Message of the Day** from the SGM Main Menu.

- Select the SGM server name in the bottom right corner of the SGM Main Window.

- SGM displays the Message of the Day dialog (Figure 18-1).

Figure 18-1   Message of the Day Dialog
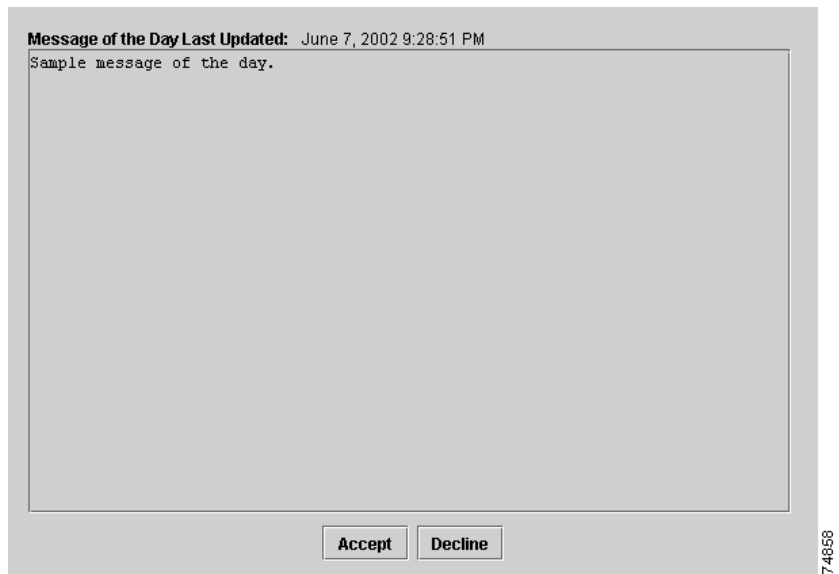
The Message of the Day dialog contains the following fields and buttons:

Field or Button	Description
Message of the Day Last Updated	Date and time the message of the day was last updated. If there is no message of the day, SGM displays **Unknown**.
Message Field	Text of the message of the day. If there is no message of the day, SGM displays **There is no message of the day**.
Accept	Closes the Message of the Day dialog and launches the client. If you do not click **Accept**, you cannot launch the client. This button is available when there is a message of the day and you launch the SGM client or GTT client.

Field or Button	Description
Decline	Closes the Message of the Day dialog and exits the client.
	This button is available when there is a message of the day and you launch the SGM client or GTT client.
OK	Closes the Message of the Day dialog without exiting the client.
	This button is available if you displayed the Message of the Day dialog by selecting **View > Message of the Day** from the SGM Main Menu.

If you want to configure SGM to display a message of the day, you must first enable the function. To do so, log in as the root user, as described in the "Becoming the Root User (Solaris Only)" section on page 2-3, or as a super user, as described in the "Specifying a Super User (Solaris Only)" section on page 18-24, then enter the following commands:

> **# cd /opt/CSCOsgm/bin**

> **# ./sgm motd enable**

SGM displays the following prompt:

> **Enter location of the message of the day file: [/opt/CSCOsgm/etc/motd]**

To accept the default value, press **Enter**; or type a different location and press **Enter**. SGM displays the following messages:

> **Setting Message of the Day File to: [/opt/CSCOsgm/etc/motd]**

> **Message of the Day File set to: [/opt/CSCOsgm/etc/motd]**

> **SGM server must be restarted for changes to take effect.**

Initially, the file is blank; enter the following command to specify the message text:

> **# ./sgm motd edit**

You can also use the **sgm motd edit** command at any time to change the text of the message of the day.

To display the contents of the message of the day file, enter the following command:

> **# ./sgm motd cat**

To disable this function (that is, to stop displaying the message of the day whenever a user attempts to launch an SGM or GTT client), enter the following command:

> **# ./sgm motd disable**

Manually Synchronizing Local SGM Passwords

If **sgm authtype** is set to **solaris**, SGM automatically synchronizes local SGM passwords with Solaris at 1:30 AM each night. However, you can also manually synchronize passwords at any time. To do so, log in as the root user, as described in the "Becoming the Root User (Solaris Only)" section on page 2-3, then enter the following commands:

> **# cd /opt/CSCOsgm/bin**

> **# ./sgm syncusers**

SGM synchronizes the passwords with Solaris.

Listing All Currently Defined Users

You can list all currently defined users in the SGM User-Based Access authentication list. To do so, log in as the root user, as described in the "Becoming the Root User (Solaris Only)" section on page 2-3, or as a super user, as described in the "Specifying a Super User (Solaris Only)" section on page 18-24, then enter the following commands:

> **# cd /opt/CSCOsgm/bin**

> **# ./sgm listusers**

SGM displays the following information for each user:

- User name

- Last time the user logged in

- User's authentication access level

- User's current authentication status, such as **Account Enabled** or **Password Disabled**

To list information for only a specific user, enter the following command:

>**# ./sgm listusers** *username*

where *username* is the name of the user.

Note You can also view user account information on the SGM User Accounts Web page. For more information, see the "Viewing SGM User Account Information" section on page 21-47.

Displaying the Contents of the System Security Log

You can display the contents of the system security log with PAGER. To do so, log in as the root user, as described in the "Becoming the Root User (Solaris Only)" section on page 2-3, or as a super user, as described in the "Specifying a Super User (Solaris Only)" section on page 18-24, then enter the following commands:

>**# cd /opt/CSCOsgm/bin**

>**# ./sgm seclog**

The following security events are recorded in the log:

- All changes to system security, including adding users

- Login attempts, whether successful or unsuccessful, and logoffs

- Attempts to switch to another user's account, whether successful or unsuccessful

- Attempts to access files or resources of higher authentication level

- Access to all privileged files and processes
- Operating system configuration changes and program changes, at the Solaris level
- SGM restarts
- Failures of computers, programs, communications, and operations, at the Solaris level

To clear the log and restart the server, enter the following command:

 # ./sgm seclog clear

The default path and filename for the system security log file is */opt/CSCOsgm/logs/sgmSecurityLog.txt*. If you installed SGM in a directory other than */opt*, then the system security log file is located in that directory.

> **Note** You can also view the system security log on the SGM System Security Log Web page. For more information, see the "Viewing the SGM System Security Log" section on page 21-41.

Restoring Security-Related SGM Data

If you inadvertently delete your user accounts, or make other unwanted changes to your SGM security information, SGM enables you to restore the security-related parts of the SGM data files from the previous night's backup.

To restore the files, log in as the root user, as described in the "Becoming the Root User (Solaris Only)" section on page 2-3, then enter the following commands:

 # cd /opt/CSCOsgm/bin

 # ./sgm restore security

SGM restores the files.

Disabling SGM User-Bases Access

For some reason, you might want to completely disable SGM User-Based Access. To do so, log in as the root user, as described in the "Becoming the Root User (Solaris Only)" section on page 2-3, or as a super user, as described in the "Specifying a Super User (Solaris Only)" section on page 18-24, then enter the following commands:

> **# cd /opt/CSCOsgm/bin**

> **# ./sgm useraccess disable**

SGM User-Based Access is disabled the next time you restart the SGM server, using the following command:

> **# ./sgm restart**

Specifying a Super User (Solaris Only)

SGM enables you to specify one or more *super users*. A super user can perform most functions that otherwise require the user to be logged in as the root user. (The root user can still perform those functions, too.) If you specify a super user, the server also runs as the super user and not as the root user.

⚠

Caution   As a super user, you can adversely affect your operating environment if you are unaware of the effects of the commands you use. If you are a relatively inexperienced UNIX user, limit your activities as a super user to the tasks described in this document.

To specify a super user, log in as the root user, as described in the "Becoming the Root User (Solaris Only)" section on page 2-3, then enter the following commands:

> **# cd /opt/CSCOsgm/bin**

> **# ./sgm superuser** *username*

where *username* is the name of the user.

When you specify a super user, keep in mind the following considerations:

- The user must exist in the local */etc/passwd* file. You cannot specify a user that is defined in a distributed Network Information Services (NIS) system.

- The super user does not have access to all SGM commands. You must still be logged in as the root user to enter the following commands:

  - **sgm backup**
  - **sgm browserpath**
  - **sgm certgui**
  - **sgm certtool**
  - **sgm clean**
  - **sgm cleanall**
  - **sgm cleandb**
  - **sgm cw2ksetup**
  - **sgm evilstop**
  - **sgm jspport**
  - **sgm keytool**
  - **sgm killclients**
  - **sgm reboot**
  - **sgm restore**
  - **sgm restoreprops**
  - **sgm setpath**, if you are specifying a *username*
  - **sgm ssl**
  - **sgm sslstatus**
  - **sgm stopclients**
  - **sgm superuser**
  - **sgm syncusers**
  - **sgm telnetpath**
  - **sgm trapsetup**
  - **sgm uninstall**

- **sgm webport**

- **sgm xtermpath**

- If **sgm authtype** is set to **solaris**, you must still be logged in as the root user to enter the following commands:

  - **sgm adduser**

  - **sgm disableuser**

  - **sgm enableuser**

  - **sgm updateuser**

- If the SNMP trap port number on the SGM server is less than 1024, you cannot use the **sgm superuser** command. To correct this situation, you must specify a new SNMP trap port number that is greater than 1024:

  - To change the SNMP trap port number in the ITPs in your network, use the **snmp-server host** command. By default, SGM listens for traps from trap multiplexing devices and NMS applications on port 44750, so that is a good port number to choose. The SNMP trap port number must be the same on all ITPs in your network.

  - See the description of the **snmp-server host** command in the "ITP Requirements" section of the *Cisco Signaling Gateway Manager Installation Guide* for more information.

  - Use the **sgm trapsetup** command to change the SNMP trap port number in the SGM server to match the port number in the ITPs in your network. See the "sgm trapsetup" section on page C-122 for more information.

Implementing SSL Support in SGM

You can implement Secure Sockets Layer (SSL) support in your SGM system. When you do so, SGM uses secure sockets to encrypt all communication between the SGM clients and server.

This section includes the following information:

- Enabling SSL Support in SGM, page 18-27

- Downloading the SGM Server's Self-Signed SSL Certificate, page 18-30

- Launching the SGM Certificate Tool for SSL, page 18-31

Enabling SSL Support in SGM

To enable SSL support in SGM, perform the following tasks:

Step 1   Obtain the SSL-enabled version of SGM.

Due to US government restrictions on the export of SSL-enabled software, Cisco provides two versions of SGM: Basic SGM, which does not provide SSL support, and SSL-enabled SGM, which does.

To obtain SSL-enabled SGM, you must contact Cisco TAC or your Cisco Account Team. They will help you apply for an export licence and download and install SSL-enabled SGM.

Step 2   Install an SSL key/certificate pair in SGM, using one of the following procedures:

- To install a new SSL key and a self-signed certificate, generate the key and certificate by logging in as the root user on the SGM server and entering the **sgm keytool genkey** command.

    SGM stops the SGM server and issues the following prompts:

    ```
    Country Name (2 letter code) []:
    State or Province Name (full name) []:
    Locality Name (eg, city) []:
    Organization Name (eg, company) []:
    Organizational Unit Name (eg, section) []:
    Common Name (your hostname) []:
    Email Address []:
    ```

    Enter the requested information.

SGM generates the following files:

- – */opt/CSCOsgm/etc/ssl/server.key* is the SGM server's private key. Ensure that unauthorized personnel cannot access this key.

- – */opt/CSCOsgm/etc/ssl/server.cer* is the self-signed SSL certificate.

- – */opt/CSCOsgm/etc/ssl/server.csr* is a certificate signing request (CSR). It is not used if you are using a self-signed SSL certificate.

- To install a new SSL key and a CA-signed certificate, generate the key and a CSR by logging in as the root user on the SGM server and entering the **sgm keytool genkey** command.

  SGM stops the SGM server and issues the following prompts:

```
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (your hostname) []:
Email Address []:
```

  Enter the requested information.

  SGM generates the following files:

  - – */opt/CSCOsgm/etc/ssl/server.key* is the SGM server's private key. Ensure that unauthorized personnel cannot access this key.

  - – */opt/CSCOsgm/etc/ssl/server.csr* is a CSR.

  - – */opt/CSCOsgm/etc/ssl/server.cer* is the self-signed SSL certificate. It is not used if you are using a CA-signed SSL certificate; the CA-signed certificate overrides the self-signed certificate.

  Print the CSR in X.509 format, by logging in as the root user on the SGM server and entering the **sgm keytool print_csr** command.

  Send the CSR to a certificate authority (CA) to be signed.

  After the CA signs the certificate, log in as the root user on the SGM server and enter the following command:

  # ./sgm keytool import_cert *cert_filename*

  where *cert_filename* is the name of the signed certificate.

  SGM stops the SGM server and imports the certificate in X.509 format.

- To use an existing signed key/certificate pair, log in as the root user on the SGM server and enter the following command:

    # ./sgm keytool import_key *key_filename cert_filename*

    where *key_filename* is the name of the existing SSL key and *cert_filename* is the name of the existing signed certificate.

    SGM stops the SGM server and imports the SSL key in OpenSSL format and the signed SSL certificate in X.509 format.

Step 3   Enable SSL support in SGM, by logging in as the root user on the SGM server and entering the **sgm ssl enable** command.

Step 4   Set up the SGM client-side SSL certificate trust relationship, by downloading and importing the self-signed or CA-signed certificate on every remote SGM client, Windows as well as Solaris, that connects to the SGM server.

   a.   (Self-signed certificate only) Download the self-signed certificate (*server.cer*), using the procedure in the "Downloading the SGM Server's Self-Signed SSL Certificate" section on page 18-30.

   b.   Import the self-signed or CA-signed certificate, using the procedure in the "Importing an SSL Certificate to an SGM Client" section on page 18-33.

Step 5   Restart the SGM client.

The SGM clients can now connect to the SGM server using SSL. All communication between the server and clients is encrypted.

If an SGM or GTT client that is not SSL-enabled attempts to connect to an SSL-enabled SGM server, SGM displays an appropriate warning message and opens the SGM client download page. The user can then download and install a new SGM client to use to connect to that SGM server.

If the client is SSL-enabled but does not have the correct certificate, SGM displays an appropriate warning message and opens the SGM Server SSL Certificate page. The user can then download the signed SSL certificate in X.509 format to the client.

Downloading the SGM Server's Self-Signed SSL Certificate

If you have implemented Secure Sockets Layer (SSL) support in your SGM system, you can download the SGM server's signed SSL certificate to all remote SGM clients that connect to the server using SSL.

To download the certificate from the SGM Server SSL Certificate page, use the following procedure on each remote SGM client:

Step 1 Use one of the following procedures to access the SGM Server Home Page:

- Select **View > SGM Server > Home Page** from the SGM Main Menu.

- Enter the following URL in a Web browser:

  https://*server_name***:***1774*

  where *server_name* is the name or IP address of the server on which the SGM server is running and *1774* is the Web port being using by SGM. (**1774** is the default port number.) If you do not know the name or Web port of the SGM Web Server, contact the system administrator who installed the SGM server software.

  SGM displays the SGM Server Home page.

Step 2 Select **Server SSL Certificate** from the SGM Server Home Page. SGM displays the SGM Server SSL Certificate page.

Step 3 Right-click **Download SGM Server SSL Certificate**.

Step 4 Select **Save Link As** from the right-click menu.

Step 5 Select a directory in which to save the certificate (*server.cer*), and click **Save**. SGM downloads the *server.cer* file into the specified directory.

Launching the SGM Certificate Tool for SSL

If you have implemented Secure Sockets Layer (SSL) support in your SGM system, you can launch the SGM Certificate Tool for SSL. The SGM Certificate Tool dialog lists all SSL certificates that have been imported by the SGM client, and enables you to import, export, and display detailed information about SSL certificates.

To launch the SGM SSL Certificate Tool, use one of the following procedures:

- In Solaris, log in as the root user and enter the following commands:
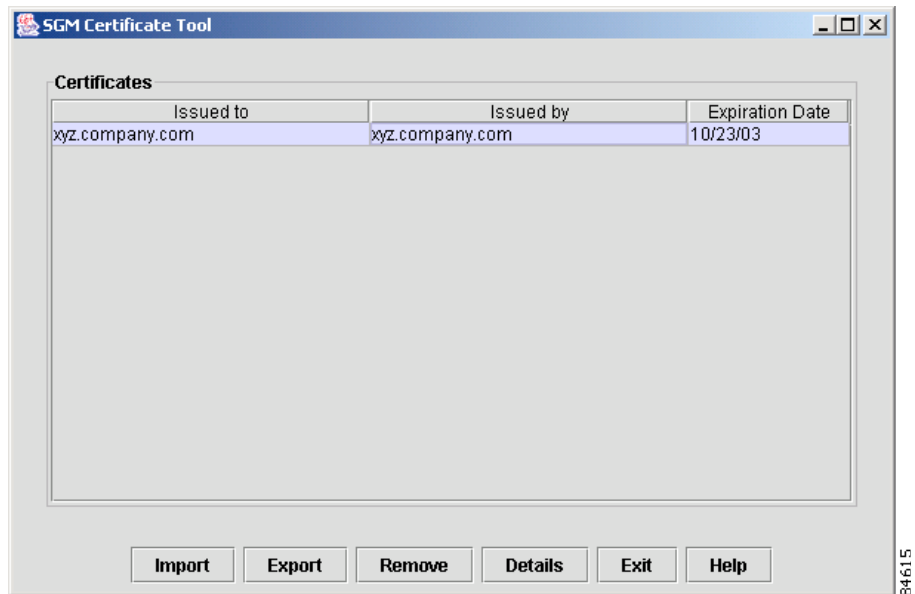
    # cd /opt/CSCOsgm/bin

    # ./sgm certgui

    See the "sgm certgui" section on page C-15 for more information.

- In Windows, select **Start > Programs > Cisco SGM Client > SGM SSL Certificate Tool**.

SGM displays the SGM Certificate Tool dialog (Figure 18-1).

Figure 18-2   SGM Certificate Tool Dialog

The SGM Certificate Tool dialog displays the following information about each SSL certificate:

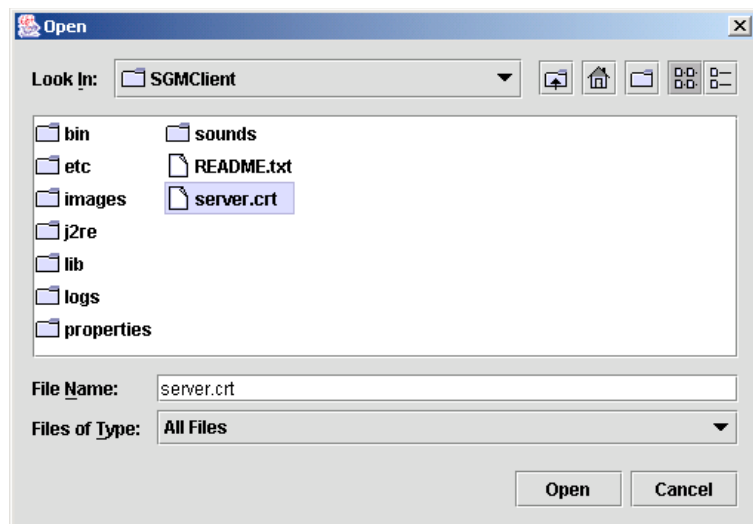| Field or Button	Description
Issued to	Host name of the SGM server to which the SSL certificate was issued.
Issued by	Certificate authority (CA) that issued the SSL certificate. Self-signed SSL certificates display the host name of the SGM server.
Expiration Date	Date on which the SSL certificate expires.
Import	Displays the Open dialog for an SSL certificate, which enables you to import SSL certificates.
Export	Displays the Save dialog for an SSL certificate, which enables you to export the selected SSL certificate.
Remove	Removes the selected SSL certificate from the table.

Field or Button	Description
Details	Displays the Certificate Information dialog, which provides detailed information about the selected certificate.
Exit	Closes the SGM Certificate Tool dialog.
Help	Displays online help for the current window.

Importing an SSL Certificate to an SGM Client

If you have implemented Secure Sockets Layer (SSL) support in your SGM system, you can import the SGM server's self-signed SSL certificate, or a CA-signed SSL certificate, to all remote SGM clients that connect to the server using SSL.

To import an SSL certificate, launch the SGM SSL Certificate Tool, as described in the "Launching the SGM Certificate Tool for SSL" section on page 18-31, then click **Import**. SGM displays the Open dialog for SSL certificates (Figure 18-1).

Figure 18-3   Open Dialog for SSL Certificates

Use the Open dialog to locate the SSL certificate that you want to import. The Open dialog for an SSL certificate provides the following fields and buttons:

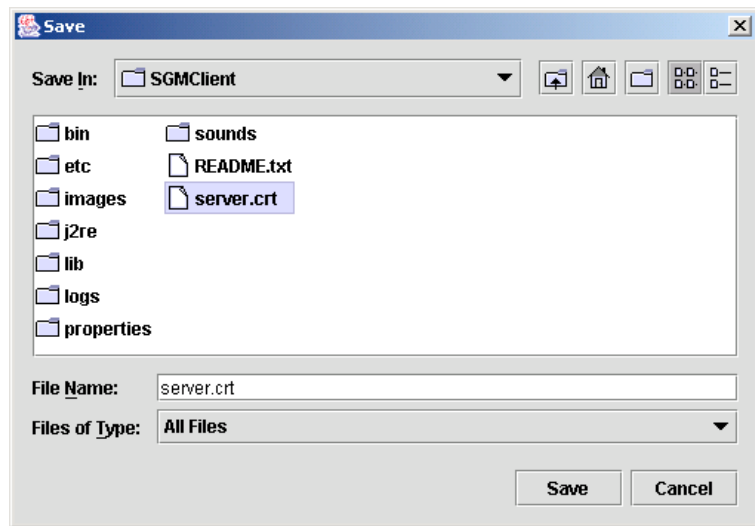| Field or Button	Description
Look In	Enables you to select the directory in which you want to find the SSL certificate. Either accept the default directory, or select a new directory from the drop-down list box. For a self-signed certificate, locate the directory in which you downloaded the certificate.
File Name	Enter a name for the SSL certificate, or select a file from those listed in the **Open** field. SGM displays the name of the certificate in the **File Name** field.
Files of Type	Specifies the type of file to display, and displays all files of that type in the selected directory. For SSL certificates, this field displays **All files**, which means files of all types are displayed in the table.
Up One Level	Displays the sub-folders and files that are in the folder that is up one level from the currently displayed folder.
Desktop	Displays the sub-folders and files that are on your workstation desktop.
Create New Folder	Creates a new sub-folder in the displayed folder.
List	Displays only icons for sub-folders and files.
Details	Displays detailed information for sub-folders and files, including their size, type, date they were last modified, and so on.
Open	Imports the file, closes the Open dialog for an SSL certificate, and populates the SGM Certificate Tool dialog with the SSL certificate's information.
Cancel	Closes the Open dialog for an SSL certificate without importing the file.

Related Topics:

- Launching the SGM Certificate Tool for SSL, page 18-31

Exporting an SSL Certificate

If you have implemented Secure Sockets Layer (SSL) support in your SGM system, you can export SSL certificates that have been imported to the SGM client.

To export an SSL certificate, launch the SGM SSL Certificate Tool, as described in the "Launching the SGM Certificate Tool for SSL" section on page 18-31, select a certificate from the list, then click **Export**. SGM displays the Save dialog for SSL certificates (Figure 18-1).

Figure 18-4   Save Dialog for SSL Certificates

Use the Save dialog to export the SSL certificate to another directory. The Save dialog for an SSL certificate provides the fields and buttons:

Field or Button	Description
Save In	Enables you to select the directory in which you want to save the SSL certificate. Either accept the default directory, or select a new directory from the drop-down list box.
	For a self-signed certificate, locate the directory in which you downloaded the certificate.
File Name	Enter a name for the SSL certificate, or select a file from those listed in the **Save In** field. SGM displays the name of the certificate in the **File Name** field.

Field or Button	Description
Files of Type	Specifies the type of file to save, and displays all files of that type in the selected directory. For SSL certificates, this field displays **All files**, which means files of all types are displayed in the table.
Up One Level	Displays the sub-folders and files that are in the folder that is up one level from the currently displayed folder.
Desktop	Displays the sub-folders and files that are on your workstation desktop.
Create New Folder	Creates a new sub-folder in the displayed folder.
List	Displays only icons for sub-folders and files.
Details	Displays detailed information for sub-folders and files, including their size, type, date they were last modified, and so on.
Save	Saves the file, closes the Save dialog for an SSL certificate, and returns to the SGM Certificate Tool dialog. Click **Exit** to close the SGM Certificate Tool dialog and export the self-signed SSL certificate in X.509 format.
Cancel	Closes the Save dialog for an SSL certificate without saving the file.

Related Topics:

- Launching the SGM Certificate Tool for SSL, page 18-31

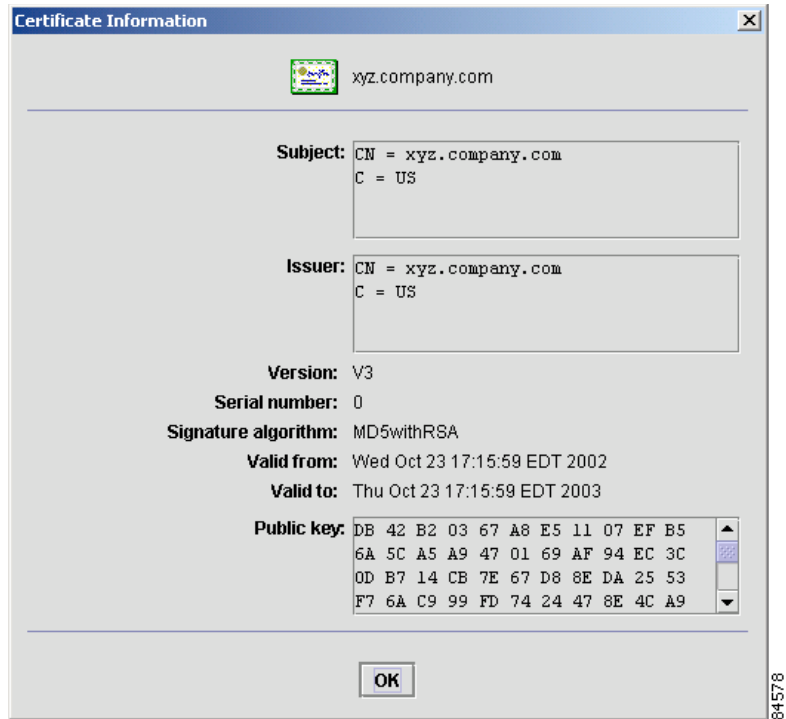# Viewing Detailed Information About an SSL Certificate

If you have implemented Secure Sockets Layer (SSL) support in your SGM system, you can view detailed information about SSL certificates that have been imported to the SGM client.

To view detailed information about an SSL certificate, use one of the following procedures:

- Click the "locked padlock" symbol in the bottom left corner of any SGM window.

- Launch the SGM SSL Certificate Tool, as described in the "Launching the SGM Certificate Tool for SSL" section on page 18-31, select an SSL certificate from the list and click **Details**.

SGM displays the Certificate Information dialog (Figure 18-1).

Figure 18-5   Certificate Information Dialog

The Certificate Information dialog displays the following detailed information for the selected SSL certificate:

Field or Button	Description
Subject	Device to which the SSL certificate was issued.
	The **Subject** field always includes the Common Name (CN) of the subject, which must match the fully qualified host name of your SGM server, such as **sgm-sun8.cisco.com**.
	The **Subject** field might also contain other information, such as the Country (C), Organizational Unit (OU), or Organization (O) of the subject.
Issuer	CA that issued the SSL certificate.
	The **Issuer** field might include the Common Name (CN) of the issuer, as well as the Country (C), Organizational Unit (OU), or Organization (O) of the issuer.
Version	Version of the SSL certificate, such as **V1**.
Serial number	Serial number associated with the SSL certificate.
Signature algorithm	Asymmetric algorithm used to ensure that the digital signature is secure, such as **MD5withRSA**.
Valid from	Date and time on which the SSL certificate was created or became valid.
Valid to	Date and time on which the SSL certificate expires.
Public key	Public key associated with the SSL certificate, used for encryption and for verifying signatures.
OK	Closes the Certificate Information dialog.
	When you are ready to close the dialog, click **OK**. SGM closes the Certificate Information dialog. If necessary, click **Exit** to close the SGM Certificate Tool dialog.

Related Topics:

-

Managing SSL Support in SGM

SGM enables you to perform the following tasks to make it easier to manage SSL support in SGM:

- To display the current status of SSL support in SGM, including whether SSL support is enabled or disabled and which SSL keys and certificates exist, use either the **sgm ssl status** or **sgm sslstatus** command.

- To print the SGM server's SSL certificate in X.509 format, use the **sgm keytool print_crt** command.

- To list the SSL key/certificate pair on the SGM server, use the **sgm keytool list** command.

- To list all SSL certificates on the SGM client, launch the SGM SSL Certificate Tool. SGM lists each imported certificate, including to whom the certificate was issued, who issued the certificate, and when the certificate expires.

See the "SGM Command Reference" section on page C-1 for more information on the use of these commands.

See the "Importing an SSL Certificate to an SGM Client" section on page 18-33 for more information on launching the SGM SSL Certificate Tool.

Disabling SSL Support in SGM

SGM enables you to disable SSL support in SGM, and to remove SSL keys and certificates from the SGM server and clients:

- To disable SSL support in SGM, use the **sgm ssl disable** command.

  See the "sgm ssl" section on page C-98 for more information.

- To remove all SSL keys and certificates from the SGM server, use the **sgm keytool clear** command. SGM stops the SGM server, if necessary, and removes the keys and certificates. Before restarting the server, you must either generate new SSL keys using the **sgm keytool genkey** command, or you must completely disable SSL using the **sgm ssl disable** command.

  See the "SGM Command Reference" section on page C-1 for more information on the use of these commands.

- To remove an SSL certificate from the SGM client, launch the SGM SSL Certificate Tool. SGM lists each imported certificate. Select the certificate you want to remove, and click **Remove**. SGM deletes the certificate from the list.

  See the "Importing an SSL Certificate to an SGM Client" section on page 18-33 for more information on launching the SGM SSL Certificate Tool.

Limiting SGM Client Access to the SGM Server (Solaris Only)

By default, when you first install SGM, all SGM client IP addresses are allowed to connect to the SGM server. However, SGM enables you to limit client access to the server by creating and maintaining the *ipaccess.conf* file.

You can create the *ipaccess.conf* file and populate it with a list of SGM client IP addresses that can connect to the SGM server. SGM allows connections from only those clients, plus the local host. If the file exists but is empty, SGM allows connections only from the local host. (SGM always allows connections from the local host.)

When you first install SGM, the *ipaccess.conf* file does not exist and SGM allows all client IP addresses to connect to the SGM server. To create the *ipaccess.conf* file and work with the list of allowed client IP addresses, use the following procedure:

Step 1   Log in as the root user, as described in the "Becoming the Root User (Solaris Only)" section on page 2-3, or as a super user, as described in the "Specifying a Super User (Solaris Only)" section on page 18-24.

Step 2   Enter the following command:

cd /opt/CSCOsgm/bin

Step 3   Create the *ipaccess.conf* file:

- To create the *ipaccess.conf* file and add a client IP address to the list, enter the following command:

    # ./sgm ipaccess add

- To create the *ipaccess.conf* file and open the file to edit it directly, enter the following command:

    # ./sgm ipaccess edit

The default directory for the file is located in the SGM installation directory:

- If you installed SGM in the default directory, */opt*, then the default directory is */opt/CSCOsgm/etc*.

- If you installed SGM in a different directory, then the default directory is located in that directory.

In the *ipaccess.conf* file, begin all comment lines with a pound sign (#).

All other lines in the file are SGM client IP addresses, with one address per line.

Wildcards (*) are allowed, as are ranges (for example, 1-100). For example, the address *.*.*.* allows all clients to connect to the SGM server.

After you create the *ipaccess.conf* file, you can use the full set of **sgm ipaccess** keywords to work with the file:

- **clear**—Remove all client IP addresses from the *ipaccess.conf* file, and allow connections from any SGM client IP address.

- **list**—List all client IP addresses currently in the *ipaccess.conf* file. If no client IP addresses are listed (that is, the list is empty), connections from any SGM client IP address are allowed.

- **rem**—Remove the specified client IP address from the *ipaccess.conf* file.

- **sample**—Print out a sample *ipaccess.conf* file.

See the for more information.

Any changes you make to the *ipaccess.conf* file take effect when you restart the SGM server.

SGM also enables you to limit the IP addresses that can send traps to the server by creating and maintaining the *trapaccess.conf* file. For more information, see the "Limiting Traps by IP Address (Solaris Only)" section on page 19-40.